## 5. INFORMATION OPERATIONS AND INFORMATION WARFARE

**[Related topics: 2.9, 2.10, 2.11, 2.35, 2.36]**

### 5.1 Information Operations Policy

- As the Air Force's information operations capabilities improve, what are the law and policy issues that need to be addressed?
- Discuss ideas about Air Force information operations organization.

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key Terms: Information Operations, law, policy

### 5.2 What is the optimum mix of systems to provide robust and reliable communications?

- Which technologies are best suited for "reachback" communications?
- Which are cheapest? Most survivable? Most reliable?
- What are the bandwidth issues?
- Which technologies are best suited to handle the last mile?
- Evaluate the potential of the following systems: laser communications, space systems, UAVs/high-altitude airships as relay, cellular systems, combat aircraft as relay.
- Is there a network architecture incorporating some or all of the above that is desirable? If so, how should such a system be developed?
- What tradeoffs should be examined in adding on-board processing to ISR and combat systems to reduce communication requirements?
- What commercial systems are likely to be available, and how does this affect this analysis? Can space assets be used as a "CRAF"-like concept?
- What are the costs, both to the military and to the civilian economy if these satellites are no longer available to their civilian customers?
- What commercial systems may be available to an adversary, and how does this affect the types of systems the US should use? What are the security implications?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key Terms: commercial space systems, satellite protection, surge capacity, CRAF, communications, imagery, remote sensing, shutter control, C2

### 5.3 What is the optimum mix of systems for potential future conflicts to provide robust and reliable surveillance, reconnaissance and gathering of intelligence?

- What are the most promising technologies for dealing with the WMD problem?
  - What is the tradeoff between air and space platforms?
- What role do ISR assets have in the spectrum of "Find, Fix, Track, Target, Engage, Assess" (F2T2EA)? In which areas of this spectrum is ISR weakest?
- Which technologies are best suited for electronic and signals intelligence? On what platforms or combination of platforms (space, high-altitude UAV, high-altitude airships, and aircraft) should these technologies be placed?

- What is the optimum mix of aircraft, UAVs, satellites, and sensors (optical, IR, laser, multi-spectral, hyperspectral) to provide surveillance and reconnaissance?
- With new radar and sensing technologies on the next generation of aircraft, is space sensing necessary?
- What systems are available to prospective adversaries? If they use these systems, can the US achieve either tactical or strategic surprise, or have we entered an era of transparency in military operations?
- How can/should the US deal with entities that use satellite or other ISR capabilities to aid adversaries?
- Can/should the US purchase all ISR capability (use "checkbook shutter control" to limit an adversary's use)? Will such a strategy always be possible?
- What are the implications of foreign investments in anti-ISR and other disruptive technologies?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key Terms: commercial space systems, satellite protection, surge capacity, CRAF, communications, imagery, remote sensing, shutter control, ISR

**5.4 How should the operations of multiple Intelligence, Surveillance, and Reconnaissance (ISR) platforms be integrated and fused?**

- What is the appropriate C2 architecture for Processing, Exploitation, and Dissemination (PED) of theater airborne ISR assets?
- Where is the best location for ISR PED—in the AOC, via Reachback ops, split-based ops, or another option?
- Is a separate architecture needed for Time-Sensitive Targeting (TST) vice non-TST?
- With limited exploitation assets—facilities, equipment, and personnel—how are the increased demands from multiple, simultaneous operations and platforms handled?
- What is the appropriate C2 structure/relationship for ISR PED assets—especially Reachback PED assets--OPCON, TACON, or Direct Support?
- How does the USAF integrate and capitalize on Joint, Coalition/Allied and Total Force ISR PED capabilities?
- How should commercial assets be better incorporated to compensate for shortfalls in military ISR capabilities or availability?
- Are 'turf battles' likely between organizations owning the various platforms?
- Is there a CRRA panel for ISR?
- Discuss warfighting integration and the CIO.

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key Terms: ISR, integration, reachback, PED

**5.5 Analyze the DOD role in protecting cyberspace for the United States.**

- Summarize existing national and DOD guidance (e.g. PDDs, national plans, DOD directives).
- Conduct a deficit analysis between infrastructure threats and existing protection programs.
- Analyze possible new approaches to protection of the national infrastructure, and how to address the threat.

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key Terms: IO, IW, NII, Defending America's Cyberspace, Homeland Defense

**5.6 What are the implications and issues surrounding IO and Homeland Defense?**

- What are the areas of IO that could have a beneficial impact on Homeland Defense?
- What are the legal and ethical limits that must be taken into consideration?
- What are the proposed procedures for implementing an IO campaign within the Homeland Defense arena?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key Terms: IO, Homeland Defense

**5.7 What unintended consequences (or "blowback") could result from the employment of computer network attacks (CNA)?**

- Would the purported deniability or non-traceability of electronic attacks prevent attacked societies from focusing on the originating country or group?
- Just as traditional US military capabilities have shown a clear progression away from mass effects against societies and toward precision effects against military capabilities, should IW policy and capabilities, if/when developed, focus on precision rather than mass information effects?
- What is the effect of large-scale CNAs that address civilian infrastructure and defense issues? What are the policy issues associated with these various scenarios?
- How does the unpredictability of the "weapon" create law of armed conflict (LOAC) issues?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key Terms: IO, IW, LOAC, law of armed conflict, unintended consequences, policy issues, CNA, blowback

**5.8 How can we improve IO in a coalition/allied environment? (Also see topic 5.14)**

- How do security concerns and improved technologies impact IO in a coalition/allied environment? What do/don't we share or disclose? How do we overcome these concerns? How does this issue relate to homeland defense?
- Do current Concepts of Operations need to be changed? How?

- How have allies such as the UK or NATO handled IO better? Examine the concept operations for allied Public Information Officers in relation to US Public Affairs Officers.
- Analyze real world and exercise examples of successes and failures of IO operating in a coalition/allied effort.

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key Terms: IO, IW, coalition, security, homeland defense

**5.9 How do we measure nation-states'/non-state entities' levels of vulnerability to IO?**

- Does the US do too much "mirror-imaging"? What models can be used to avoid errors made my mirror-imaging?
- Examine portions of a potential adversary's infrastructure. Include insights on why categories were chosen, application to other analysis, and potential interrelationships between categories.
- How do we determine the key nodes/centers of gravity (COGs) in an adversary's information infrastructure? What models are useful in determining nodes/COGs for Influence Operations?
- Compare and contrast kinetic and non-kinetic effects.

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key Terms: IO, IW, vulnerability, mirror imaging, infrastructure, COG, targeting, Influence Operations

**5.10 What are measures of effectiveness (MOEs) for IW, or one of its disciplines?**

- What are ways to measure IW contributions in terms of denying data, information, knowledge, understanding, and operational wisdom? How can this be related to achieving the commander's objective?
- How can the Unified Joint Task List (UJTL) MOEs be used as a foundation for more sophisticated MOE development?
- Can Joint Munitions Effectiveness Manuals (JMEMs) be developed for IW?
- What do commanders expect of IW and how can those expectations be measured?
- How can IW MOEs be validated?
- What are some MOE categories (e.g., planning process, programmatic, logistical, time, damage, perception management, etc.)?
- What are ways to conduct IW combat assessment (like battle damage assessment)?

POC: INSS, DSN 333-2717, Comm 719-333-2717
Priority: 1
Key Terms: IO, IW, measures of effectiveness, Unified Joint Task List

**5.11 What is the effect of international media on US military operations and on IW/IO planning?**

- Citing case studies as examples, discuss which IW/IO means were most important for a given side in a particular conflict.
- How should the AF and DOD provide international public information?
- What is the effect on the US military actions by not using the international media or having an implemented global communications strategy?
- How can IW/IO planning better involve the international media?
- What is the relationship between strategic communications and IO?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key Terms: IO, IW, media, IO planning, Kosovo, Serbia, Afghanistan, Iraq

**5.12 What is the interrelationship of themes between Public Affairs (PA), Psychological Operations (PSYOP), and Military Deception (MD)? (Also see topic 5.22)**

- What is the advantage gained by combining PA, PSYOP, MD and OPSEC under a coordinated planning effort?
- In an Information Warfare Flight or a Joint Force Commander IO Cell how are PA, PSYOP and MD themes coordinated and deconflicted effectively?
- Who are the key audiences for PA, PSYOP and MD? Is there a concept of acceptable collateral (media) damage if a message is received by the wrong audience?
- Are there any legal protections for PA, PSYOP, MD if there is collateral damage? Are there additional means for mitigating the collateral damage/legal problems?
- How can PA maintain "integrity and credibility" while working with PSYOP and MD?
- Discuss the separation between Public Affairs (counter-propaganda) aimed at a US audience vs. activities directed at foreign and/or hostile audiences
- What are the lessons learned from post 9/11 experiences in Afghanistan or Iraq that support
- Should PA remain a capability within Influence Operations?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key terms: IO, IW, deception, PSYOP, propaganda, public affairs, media, international

**5.13 Does EW belong in IO?**

- What are the operational and doctrinal considerations?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key terms: IO, IW, EW, electronic warfare, doctrine

**5.14 How can the Air Force develop PSYOP capabilities and integrate them into a Joint IO environment? (Also see topic 5.8)**

- What are the Air Force's goals in developing further PSYOP capabilities?
- What is the best means for the AF to ensure JPOTF takes Air-centric IO/PSYOP requirements (themes) into consideration?
- How can Commando Solo be better utilized as a non-SOF IO platform vs. a SOF PSYOP platform?
- What AF educational requirements can be created to ensure better PSYOP and Joint integration?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key Terms: IO, IW, PSYOP, JPOTF, Commando Solo, education.

**5.15 What are the ramifications of hostile IO/IW threats to the US, its forces, and allies?**

- Analysis of key strategic and operational IW threats to the US past and present.
- Include nation-state and non-state-entity operations.
- Possible deterrence of such activity.
- Future implications.
- Include case studies.

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key Terms: IO, IW, deterrence, anti-US, political-military, public diplomacy, terrorism

**5.16 What are some important considerations for building an IW capable force? (Also see topic 5.27)**

- Examine Total Force capabilities.
- Should a person be trained in all aspects of IW or should they specialize?
- What is the proper training for Influence Operations and Effects-Based Operations?
- Should we train to Joint or Service standards/doctrine?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key Terms: IO, IW, information warrior, standards, training, entrance testing and exams, AFSCs, Air Force Reserves (AFR), Air National Guard (ANG), ARC

**5.17 Are all Information Operations in essence Influence Operations with the common goal of gaining and maintaining an influence effect?**

- Does the AF IO Doctrine adequately define IO?
- What is a workable definition of Influence Operations?
- What are the appropriate military elements of Influence Operations for Air Force Operations (Military Deception, PSYOP, OPSEC, PA)?
- Are Joint definitions the best approach to IO?
- Is Air Force doctrine compatible with Joint concepts?

- Are Influence Operations more appropriately at the top of the hierarchy (of Information Operations) with Electronic Combat Operations (EW) and Network Operations (CNO) as subordinate mission areas within a measurable environment (Electromagnetic Spectrum and Cyberspace)?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 2
Key Terms: IO, IW, EW, CNO, OPSEC, MILDEC, PSYOP, PA, Targeting, Influence Operations

**5.18 Higher level IO effects include actions to Destroy, Deny, Degrade, Disrupt, Deceive or Usurp targets. What are key considerations that must be planned for to synchronize and deconflict those effects?**

- What is the definition or unintended consequences or "blowback" in relation to IO actions?
- How can Intelligence Gain/Loss considerations be factored into the targeting process to best serve the needs of both ISR personnel and targeteers?
- What collateral damage considerations are unique to IW? Consider non-kinetic/non-lethal options.
- How important is the consideration of compromising a special capability to the IW campaign? Is their a risk-analysis model that can be applied to use of special capabilities to mitigate compromise?
- How can IW effects be embedded in the ATO to insure integration and to comply with the concept of parallel and simultaneous operations? Is the use of a "shadow" IO Tasking Order valid to protect use of IW capabilities, but to synchronize IW effects with kinetic ATO events?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 2
Key Terms: IO, IW, EBO, ATO, C2W, targeting, ISR, Influence Operations

**5.19 How does IO contribute to full-dimensional force protection (critical nodes of personnel, facilities, equipment and technologies)?**

- What new critical infrastructure protection processes/procedures/measures need to be introduced to counter the possibility of hostile activity?
- What IW-related analytical or decision-making tools does the air commander require to ensure force protection?
- What commercial off-the-shelf (COTS) or emerging technologies, media resources, and human factors analysis would enhance force protection efforts?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 2
Key Terms: IO, IW, force protection, COTS, human factors, media

**5.20 What tools do commanders need to conduct IW at each level (Service component, JTF, Combatant Commander)?**

- How are the tools linked together? How could/should other links be made?
- Discern commanders' requirements for automated or semi-automated IW mission planning tools and common operating pictures (COPs).
- What tools would help ensure that the commander is considering all targeting options (kinetic/nonkinetic, lethal/nonlethal)?
- How can advanced technology, human factors, and human computer interaction understanding be used to enhance these tools?
- How can the need for these tools be translated into operational and acquisition requirements?
- How can education and training programs be used to effectively integrate these tools with force protection and other related base operations?
- How can visualization of IO/IW activities be most usefully integrated with other information presented to the commander?
- What measures of effectiveness would be embedded in such a visualization/map?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 2
Key Terms: IO, IW, mission planning, targeting

**5.21 How can Psychological Operations (PSYOP), using capabilities unique to the Air Force, be used most effectively in support of air, space, and cyber activities?**

- What does psychological preparation of the battlespace (P2B) entail, from both an operational and conceptual standpoint? How should P2B be conducted at the strategic, operational, and tactical levels?
- How can PSYOP be folded into the target development and selection process in support of joint or combined air combat operations? How does PSYOP fit into the effects-based operational framework? What is the Air Force role in the JPOTF of tomorrow?
- What role(s) should PSYOP expeditionary teams (PETs) play during air contingencies and EAF deployments?
- What is the synergy between PSYOP and human-factors analysis? How can this synergy best be achieved and optimized? What commercial off-the-shelf (COTS) or emerging technologies could be harnessed to enhance PSYOP capability?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 2
Key Terms: IO, IW, aerospace PSYOP, P2B, PETs, human factor analysis, COTS, Influence Operations.

**5.22 What should the role of public affairs (PA) be in IW? (Also see topic 5.12)**

- The Air Force Chief of Staff has directed PA participation in IW Flights (IWF). What role should PA have in these Flights?
- How will PA contribute to the synergism of IW?
- Examine PA/Command IW relationships.

- What type of "public affairs strategy" should we pursue in respect to defending the national infrastructure, DOD and AF against potential IW attacks?
- What type of public affairs strategy should be created to educate the public in the consequences of attack? Examples might include: crashing the FAA air traffic control network (possibly bringing down airliners filled with innocent civilians); shutting down the US power grid (causing civilian casualties); interfering with 911 networks, sending emergency vehicles to the wrong locations?
- What is the role of AF public affairs in cases where general attacks against civilian infrastructure impacts AF operations?
- What are some strategies that PA could employ to become more proactive rather than reactive?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 2
Key Terms: IO, IW, public affairs, PSYOP, information infrastructure.

**5.23 How should IW address the risk management issue for IO preparation of the battlespace (IOPB)?**

- Is risk management properly addressed in current IW TTPs? What changes if any are needed?
- How do we determine the level of acceptable risk?
- Are current Multidisciplinary Vulnerability Assessments (MDVA) acceptable tests to determine if risk management procedures are appropriate?
- Do the Operational Risk Management procedures used to design the INFOCON process also apply to the other disciplines of defensive counter information?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 2
Key Terms: IO, IW, defensive counter-information, risk management, IO vulnerabilities, TTPs, operational planning, Multidisciplinary Vulnerability Assessments, IOPB

**5.24 Explore the concept of computer network exploitation (CNE)/"Active Defense"/responsive action.**

- Define concept of CNE/"active defense" in cyber-warfare and how it is distinguished from related CND, Computer Network Attack (CNA), and Info Assurance activities.
- What advantages does having authorization and capability to conduct CNE/"active defense" as part of CND provide? What are the implications of not having authority?
- What policy and legal considerations apply to CNE/"active defense" and the establishment of ROE for its prosecution?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 2
Key Terms: IO, IW, CNE, active defense, legal, cyber-warfare

**5.25 What lessons can be learned from the private sector regarding defensive IW? (Also see topic 5.44)**

- What are the similarities and differences in the challenge of protecting the information resources of globally dispersed operations?
- How does a large, geographically dispersed organization identify, protect, and defend its most critical information assets?
- What is the best mix of centralized/decentralized protection and reserve/backup paths and systems in defending the most critical information assets?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 2
Key Terms: IO, IW, defensive IW, lessons learned, private sector, commercial

**5.26 How can DOD and the Air Force go beyond computer-focus within the Information Condition (INFOCON) system to a full-spectrum IW focus?**

- Is it possible to broaden scope so widely?
- What is the utility of moving to a full-spectrum focus?
- What organizational relationships need to be formed to make this happen?
- What are the necessary reporting chains and means to ensure compliance?
- What indications and warning data are necessary to expand to a full-spectrum threat condition?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 2
Key Terms: IO, IW, INFOCON

**5.27 Examine the possible roles and responsibilities of Air National Guard and Air Force Reserve units in IO. (Also see topic 5.16)**

- What IO roles and missions should the reserve components assume? (Include homeland defense missions in the analysis.)
- What units might be formed or slots created which will enable the United States to better utilize its IO-trained resources?
- How can their capabilities be better integrated into Total Force capabilities?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 2
Key Terms: IO, IW, Air National Guard, ARC, Reserve, National Guard

**5.28 IO is conducted across all battlespaces. What type of organizational structure is best suited to accomplish the IO mission?**

- Who should have the national IO lead?
- How do you best integrate and synchronize the diplomatic, informational, military, and economic (DIME) aspects?
- How does the Interagency Working Group structure feed the Joint Force Commander IO Cell? How does it feed Strategic Command?

- Should there be a new model for conducting IO, such as an "IO Combatant Commander," MAJCOM, or IO Task Force? What roles would each organization have? What should the organization look like?
- How does Strategic Command conduct command and control of IO? Who has the decision authority for CNA, PSYOP, and Special Information Operations? How does this organization interact with the Services? What would be their individual responsibilities?
- How should IO be addressed on the Air Staff?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 2
Key Terms: IO, IW, force structure, information infrastructure, C2, command and control, Strategic Command

**5.29 What are the implications of international treaties and agreements in the IW realm?**

- Article 5 of the North Atlantic Treaty says that "an armed attack against one or more of them in Europe or North America shall be considered an attack against them all." How does this relate to cyber attacks?
- How would an equitable arms control agreement be defined? What benefits might accrue? How are USAF equities protected?
- How are other IW powers' technological advances anticipated and addressed?
- What arms control mechanism(s) and forum/fora would be most appropriate for IW arms control? Is it possible to track/identify foreign IO/IW technology capabilities?
- How would the US Government identify, vet, and publish such a foreign "IW Militarily Critical Technologies List?" Given the short life cycle and rapid evolution of IO technologies, is this feasible given the existing bureaucratic processes?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: IO, IW, arms control, CNA, CND, IW agreements, critical technologies, proliferation

**5.30 How will evolving IO affect traditional deterrence and escalation dilemmas during international crises?**

- What advantages does information dominance give during crisis negotiations?
- How have information advantages been used to intimidate crisis adversaries?
- Does information asymmetry make escalation to war more/less likely?
- Do evolving IO make it more/less difficult for civilian principals to control military affairs under crisis conditions?
- What role can IO play in improving international crisis outcomes?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: IO, IW, Crisis management, deterrence, escalation

**5.31 What is the relationship between cyberspace and IO?**

- What are the implications for the Air Force?
- What is the appropriate division of responsibilities between the national level and the DoD?
- Does the nation need a separate cyber force?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: IO, IW, Doctrine

**5.32 How will continuing rapid changes in technology affect IO?**

- How will changes in global telecommunications, embedded devices, increasing bandwidth, etc., affect the use of IW by potential adversaries?
- How will the increasing pace of technological change affect our ability to defend against IW? How should these improved technologies be used in conjunction with our allies? What concerns exist regarding foreign military sales or the possible compromise of technology?
- Bandwidth limitations have traditionally constrained information delivery to warfighters. With increasing bandwidth available, what useful information should be added and what are ideas for displaying information more intuitively? Should some of the new bandwidth be spent to strengthen encryption?
- What is the impact on availability, integrity, authentication, confidentiality, and non-repudiation of information?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: IO, IW, advanced technology, technology forecasts, technology

**5.33 How will continuing rapid changes in human factors analysis affect IW?**

- How can new precision profiling techniques, including speech pattern analysis, lie detection, etc., be used in deception and psychological operations campaigns?
- Are resources being provided to do analysis of low level target individuals and groups (as well as high profile targets) using classified sources? Is that information immediately available to end users?
- How can cultural studies assist IO campaigns?
- Address the use of human conditioning for exploitation of EW, CNA, OPSEC.

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: IO, IW, human factors analysis, behavioral analysis, EW, PSYOP.

**5.34 What constitutes an IO campaign? For us and/or against us?**

- Does IO/IW conditioning of adversaries and allies improve the pre-hostilities environment?
- Is it possible to determine specific start and stop dates, or is IW continuous?
- How is the end-state defined in an IW campaign?

- Should there be an IW task force set up?
- What are the phases of an IW campaign? Where do they synchronize with conflict operations?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: IO, IW, campaign end, end state, task force

**5.35 Examine the traditional concepts of maneuver and firepower as they relate to cyberspace.**

- By changing addressing schemes, communications protocols, and their means, the cyberspace location of assets can be changed. Such changes offer the opportunity for maneuver in cyberwarfare.
- How can maneuver concepts improve AF/DOD ability to conduct computer network defense (CND)?
- How can one measure the disruptive effects of defensive maneuver on AF/DOD ability to communicate?
- What would constitute "firepower" in cyberspace?
- Can the synergy between maneuver, firepower, and deception that is found in the physical battlespace be replicated in cyberspace?
- How do maneuver and firepower concepts in cyberspace relate to those in other realms?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: IO, IW, cyberspace, maneuver, space

**5.36 How can the USAF IO and information technology capabilities be applied best in environments associated with asymmetric warfare or humanitarian operations?**

- Apply real world case studies and multiple analytic approaches in addressing this issue. Address successes and failures as appropriate.
- Do our current TTPs, CONOPS, etc., correctly address how we should apply IW during conflict?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: IO, IW, MOOTW, SSC, Kosovo, aerospace power, Mogadishu, Afghanistan

**5.37 How do our efforts to operate in and control cyberspace and information relate to operations in other global commons?**

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: IO, IW, space, ocean, freedom of navigation

**5.38 Compare Economic, Political, and Religious media reports in the Western and Muslim media. Can the Muslim Arab/Arab media be useful to in supporting US policies and objectives?**

- Does the Army's SCAME process offer an effective means of pursuing these options?
- Compare Arab Arab/Muslim media reaction to critical US policy/strategy plans.
- What have been the repercussions of US reactive responses to Arab/Muslim media?
- Compare the credibility and effectiveness of Muslim media with the regional audience, the US audience, and the world audience.
- Can US media be a positive force in Arab/Muslim relations?
- Would Arab/Muslim lead reporters and anchors improve the US image and assist US objectives?
- How do AF efforts fit in with DOD and national efforts to conduct international public information efforts and ensure national will in support of USG policies and objectives?
- How do AF commanders use public affairs and linkages to IW capabilities to negate or mitigate the negative impact of adversary propaganda on AF personnel?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key terms: IO, IW, propaganda, public affairs, international

**5.39 Construct an IO roadmap for QDR 2010.**

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: IO, IW, Quadrennial Defense Review, emerging threats, transformation

**5.40 What is the best structure for providing IW support to a NAF commander?**

- How do embedded IW personnel within the Air Operations Center interface with the Air Force Computer Emergency Response Team (AFCERT)?
- What is the AOC interface with the Joint IO Cell and Joint Task Force-Computer Network Operations?
- What are the roles and responsibilities of the services vs. STRATCOM?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: IO, IW, NII, Defending America's Cyberspace, homeland defense, AOC

**5.41 Conduct a system dependency analysis of network centers of gravity for cyberspace.**

- Examine interdependencies within a network
- Evaluate interdependencies with systems that are key to network operations/

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: COG, network relationships, key nodes

**5.42 Model the effects of an IO attack.**

- Create a set of measures for evaluating an attack.
- Identify methods of monitoring attack effects.
- Develop a restoration strategy/policy.
- Examine the transition from risk management to consequence management.

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: CM, BDA, assessment, effects, IO, CNA, CND, modeling, simulation

**5.43 Examine cyber exercise planning.**

- Consider cyberwarfare as an element of a larger exercise vs a cyber-focused exercise.
- Evaluate how useful past cyber exercises have been.

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: modeling, simulation, wargame, tabletop, exercises

**5.44 Examine how commercial information operations practices can be leveraged for military information. (Also see topic 5.25)**

- Identify effective bandwidth management techniques.
- Evaluate the effectiveness of acquisition processes for meeting IO requirements, given the rapid pace of technological advancement.
- Examine methods of ensuring configuration control within a network.
- Evaluate methods of networked collaboration that might facilitate battle management in cyberspace.
- Consider how to best ensure authentication and integrity of data in a network environment.

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: private industry, IA, information assurance, 5 pillars, resource management